APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

APPARATUS AND METHOD OF PROTECTING MANAGEMENT FRAMES IN WIRELESS LAN COMMUNICATIONS

Inventor(s): Emily H. Qi
Jesse Walker

Prepared by: James S. Finn,
Patent Attorney

intel®
Intel Corporation
5000 W. Chandler Blvd., CH6-404
Chandler, AZ 85226-3699
Phone: (202) 607-4607
Facsimile: (202) 318-2450

"Express Mail" label number EV325529477US

BACKGROUND

[0001] Wireless networking hardware requires the use of underlying technology that deals with radio frequencies as well as data transmission. The most widely used standard is 802.11 produced by the Institute of Electrical and Electronic Engineers (IEEE). This is a standard defining all aspects of Radio Frequency Wireless networking. A subset of 802.11 is 802.11k -- Radio Resource Management. This standard focuses on the two key WLAN elements: access points (AP) and PC Cards.

[0002] Within this 802.11 standard, Management Frames, including Action Frames are used extensively; currently there are no security mechanisms to protect these Management Frames in the IEEE 802.11 standard. Thus, there is a continuing need for better ways to protect Management Frames and thus enable more secure, efficient and reliable wireless networking.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] The subject matter regarded as the invention is particularly pointed out and distinctly claimed in the concluding portion of the specification. The invention, however, both as to organization and method of operation, together with objects, features, and advantages thereof, may best be understood by reference to the following detailed description when read with the accompanying drawings in which:

FIG. 1 illustrates a prior art wireless network subject to replay attacks;

FIG. 2 illustrates a prior art wireless network subject to forgery attacks;

FIG. 3 is a diagram of the negotiation between an access point (AP) and wireless station (STA) which utilizes the protection-capable and non-protection-Capable mechanisms of the present invention;

FIG. 4 illustrates the TKIP MPDU Format utilized in one preferred embodiment of the present invention;

FIG. 5 illustrates the format of the CCMP protocol construction to protection-capable Action Frames of one preferred embodiment of the present invention; and

FIG. 6 is a flow chart of the procedure for transmitting from the wireless station (STA); and

FIG. 7 is a flow chart of the procedure of receiving at the STA.

[0004] It will be appreciated that for simplicity and clarity of illustration, elements illustrated in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements are exaggerated

relative to other elements for clarity. Further, where considered appropriate, reference numerals have been repeated among the figures to indicate corresponding or analogous elements.

DETAILED DESCRIPTION

[0005] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will be understood by those skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known methods, procedures, components and circuits have not been described in detail so as not to obscure the present invention.

[0006] Some portions of the detailed description that follows are presented in terms of algorithms and symbolic representations of operations on data bits or binary digital signals within a computer memory. These algorithmic descriptions and representations may be the techniques used by those skilled in the data processing arts to convey the substance of their work to others skilled in the art.

[0007] An algorithm is here, and generally, considered to be a self-consistent sequence of acts or operations leading to a desired result. These include physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or

the like. It should be understood, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

[0008] Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as "processing," "computing," "calculating," "determining," or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, that manipulate and/or transform data represented as physical, such as electronic, quantities within the computing system's registers and/or memories into other data similarly represented as physical quantities within the computing system's memories, registers or other such information storage, transmission or display devices.

[0009] Embodiments of the present invention may include apparatuses for performing the operations herein. An apparatus may be specially constructed for the desired purposes, or it may comprise a general purpose computing device selectively activated or reconfigured by a program stored in the device. Such a program may be stored on a storage medium, such as, but not limited to, any type of disk including floppy disks, optical disks, compact disc read only memories (CD-ROMs), magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), electrically programmable read-only memories (EPROMs), electrically erasable and programmable read only memories (EEPROMs), magnetic or optical cards, or any other type of media suitable for storing electronic instructions,

and capable of being coupled to a system bus for a computing device.

[00010] The processes and displays presented herein are not inherently related to any particular computing device or other apparatus. Various general purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct a more specialized apparatus to perform the desired method. The desired structure for a variety of these systems will appear from the description below. In addition, embodiments of the present invention are not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein. In addition, it should be understood that operations, capabilities, and features described herein may be implemented with any combination of hardware (discrete or integrated circuits) and software.

[00011] Use of the terms "coupled" and "connected", along with their derivatives, may be used. It should be understood that these terms are not intended as synonyms for each other. Rather, in particular embodiments, "connected" may be used to indicate that two or more elements are in direct physical or electrical contact with each other. "Coupled" my be used to indicated that two or more elements are in either direct or indirect (with other intervening elements between them) physical or electrical contact with each other, and/or that the two or more elements co-operate or interact with each other (e.g. as in a cause an effect relationship).

[00012] It should be understood that embodiments of the present invention may be used in a variety of applications. Although the present invention is not limited in this respect, the devices disclosed herein may be used in many apparatuses such as in the transmitters and receivers of a radio system. Radio systems intended to be included within the scope of the present invention include, by way of example only, cellular radiotelephone communication systems, satellite communication systems, two-way radio communication systems, one-way pagers, two-way pagers, personal communication systems (PCS), personal digital assistants (PDA's), wireless local area networks (WLAN), personal area networks (PAN, and the like).

[00013] Types of cellular radiotelephone communication systems intended to be within the scope of the present invention include, although not limited to, Code Division Multiple Access (CDMA) cellular radiotelephone communication systems, Global System for Mobile Communications (GSM) cellular radiotelephone systems, North American Digital Cellular (NADC) cellular radiotelephone systems, Time Division Multiple Access (TDMA) systems, Extended-TDMA (E-TDMA) cellular radiotelephone systems, third generation (3G) systems like Wide-band CDMA (WCDMA), CDMA-2000, and the like.

[00014] The goal of 802.11k is to make measurements from Layers 1 and 2 of the OSI protocol stack -- the physical and data link layers -- available to the upper layers. This means that it is expected that the upper layers can and will make decisions about the radio environment and what can be accomplished in that

environment. One feature 802.11k will enable is better traffic distribution. Normally, a wireless device will connect to whatever AP gives it the strongest signal. This can lead to overload on some APs and underload on others, resulting in lowered overall service levels.

[00015] The 802.11k standard will allow network management software to detect this situation and redirect some of the users to underutilized APs.. Although those APs have weaker signals, they are able to provide greater throughput. This will produce higher speeds for both those on the original AP and the redirected users.

[00016] The Action Frame, a class 1 IEEE 802.11 Management Frame, is used to exchange radio resource measurement, radio resource requirement, network information, and network optimization control in IEEE 802.11 amendments (11k, 11h, 11e, and 11i). Action Frames contain valuable radio resource and network information and are subject to forgery. Forged Action frame messages can lead to poor performance or ignoring valid messages. However, the IEEE 802.11 standard and its amendments have defined no mechanism to protect Management Frames, such as Action Frames, from forgery.

[00017] As can be seen in FIG. 1, shown generally as 100, wireless networks without the capabilities provided by the present invention are subject to replay attacks. In this example, "good guy" wireless station (STA) 105 is in wireless communication with "good guy" access point (AP) 110. Without the apparatus, systems and methods of the present invention, "bad guy" STA or AP

115 can eaves drop and record 120 the wireless communication between AP 110 and STA 105 and playback selections 125 to AP 115.

[00018] FIG. 2 illustrates yet another problem with existing wireless networks using only Wireless Equivalent Privacy (WEP). Shown generally as 200, forgery attacks are illustrated with 802.11 header at 205, IV 210, Data 215 and ICV at 220. One possible attack, caused by the fact that Recv-Addr, Src-Addr, Dest-Addr are all unprotected, can be on packets from a STA to the AP, corrupting the Dest-Addr and the AP decrypting data and sending it to the forged destination. Another possible attack can be to create a blank message with the same number of data bytes and flip some bits and compute the ICV; XOR resulting bit-flipped message + ICV into captured message.

[00019] One embodiment of the present invention provides a mechanism to protect Management Frames, such as Action Frames, and enables Wireless Stations (STAs) to exchange Management Frames, such as Action Frames, in a secure manner. In this preferred embodiment of the present invention a new attribute of the Action Frame is created and depends on whether or not the Action Frame can be protected. This result is two classes of Action Frames: protection-capable frames and non-protection-capable Frames. By default, all Action Frame are non-protection-capable, for backward compatibility. Non-protection-capable Actions Frames will be "normal" Action Frames – protection never applied. protection-capable Action Frames can be protected and will be protected if local policy requires. For example, if the Basic Service Set (BSS) policy does not

require protected Action Frames, then STAs shall send all Action Frames without protection, including all protection-capable Action Frames.

[00020] If the BSS policy requires protected Action Frames, then a STA shall protect all protection-capable Action Frame. The STA shall not send protection-capable Action Frames at all if the peer has not agreed to protection. If the BSS policy requires protected Action Frames, then a STA shall discard any unprotected protection-capable Action Frame it receives, which includes those received before the IEEE 802.11i 4-Way Handshake completes. A STA shall never try to protect a non-protection-capable Action Frame it sends and shall discard any it receives protected

[00021] Further, a preferred embodiment of the present invention provides a new Robust Security Network (RSN) Capabilities bit "Protected Action Frames" to be added for Action Frame protection negotiation. Beacon/Probe Response source sets a bit to indicate that protection is required for all protection-capable Action Frames.

[00022] Beacon/Probe Response source clears this bit to indicate it does not support Action Frame protection or that protection is disabled. Responding STAs set the bit as the Beacon/Probe Response source sets it if they support Protected Actions Frames and clear it otherwise.

[00023] Turning now to FIG. 3, shown generally as 300, is an illustration of the negotiation details. In this preferred embodiment, access point (AP) 310 is in wireless communication with wireless station (STA) 305. The initial

communication 315 from AP with Beacon/Probe Response: RSN IE capabilities, provides that Protection Action Frame bit = 1 if AP 310 protects protection-capable Action Frames; and Protection Action bit = 0 if AP 310 does not protect protection-capable Action Frames.

[00024] Response 320 Association Request with RSN IE capabilities, provides that Protection Action bit is set as in the Beacon or Probe Response if STA 305 protects protection-capable Action Frames and sets the Protection Action bit = 0 otherwise.

[00025] An example RSN IE Protected Action Frame Subfield Specified BSS policy may be:

- AP sets to 0 if Protected Action Frames not supported/enabled
- AP sets to 1 if Protected Action Frames supported and enabled
- STA sets to 0 if doesn't support Protected Action Frames
- STA sets to value set by AP if it supports Protected Action Frames

However, it is understood that numerous policies can be implemented in the present invention.

[00026] Once STAs negotiation is finished, the protection-capable Action Frame is protected in the same ways as an ordinary data MPDU if local policy requires the protection-capable Action Frame to be protected. FIG. 4, shown generally as 400, illustrates the TKIP MPDU Format, with header part 405 and data frames 410. An expanded view of data frames 410 is shown by reference numerals 415 – 435, with IV/KeyID (4 octets) 415, Extended IV (4

octets) 420, Data (> = 1 octets) 425, MC (8 octets) 430 and ICV (4 octets) 435. The encrypted portion 412, includes Data 425, MC 430 and ICV435. An expanded view of IV/Key ID 415 is illustrated at 440 and 445; and an expanded view of Extended IV is illustrated at 450.

[00027] Another method of protection is accomplished by applying the IEEE 802.11i CCMP protocol construction to protection-capable Action Frames. FIG. 5, shown generally as 500, illustrates the CCMP MPDU Format of one preferred embodiment of the present invention. Header part is illustrated at 505 and data portion at 510. The data portion 510 is expanded to show IV/Key ID (4 octets) 515, Extended IV (4 octets) 520, Data (Octets > = 0) 525, and MIC (8 octets) 530. IV/Key ID 515 is shown expanded at 535 and Extended IV is expanded at 540.

[00028] The CCMP Message Integrity Code protects the Action Frame from undetected forgery. The CCMP Sequence Number protects the Action Frame from replay. The CCMP encryption scheme maintains the Action Frame payload as confidential. Sender's Pairwise Temporal Key protects unicast Action Frame and Sender's Group Temporal Key is used to protect broadcast/multicast Action Frame. An important benefit of the present invention allows the same keys that are used for data and thus no additional key management scheme required.

[00029] FIG. 6, at 600, is a flow chart of the procedure for transmitting from a wireless station (STA). At 605 the Management Frame is generated and at 610 the determination as to whether or not the Management Frame is protection-

capable is made. If it is not protection-capable, the normal Management Frame is transmitted at 640. If the Management Frame is protection-capable, at 615 it is determined if a pair of STAs agree to protect the protection-capable Management Frame. If no, at 640 again the normal Management Frame is sent. If yes, at 620 the determination as to whether or not the Unicast Key and Multicast key are in place is made. If no, at 630 there is an error and exiting occurs. If yes, then encryption of the Management Frame takes place at 625, resulting in a protection Management Frame at 635.

[00030] FIG. 7, at 700, is a flow chart of the procedure of receiving at the STA. At 705 receipt of a Management Frame occurs at a STA. At 710 it is determined if a pair of STAs agree to protect the protection-capable Management Frame. If no, the determination is made at 720 as to whether or not the Management Frame is a protected Management Frame. If yes, at 735 the current protected Management Frame is ignored or an error occurs. If yes at 710, then it is determined at 715 as to whether or not the Management Frame is a protected Management Frame. If no, at 730 it is determined if the current Management Frame is a non-protection capable Management Frame. If yes, than it is received as a normal unprotected Management Frame. If yes at 715, than at 725 the determination is made as to whether or not the Unicast Key and Multicast Key are in place. If no, than at 750, the protected Management Frame is ignored or an error occurs. If yes, at 725 the protected Management Frame is decrypted at 740. Then, at 742, the decryption result is checked to see if it was successful. If the

decryption failed for any reason, e.g., a message integrity or message sequencing error, then the frame is ignored or an error occurs. If the decryption succeeds, at 745 the determination is made as to whether or not the current Management Frame is a protection-capable Management Frame. If no at 745, than at 750 the protected Management Frame is ignored or an error occurs. If yes at 745, than it is a normal unprotected Management Frame at 755.

[00031] Thus, the present invention as articulated above describes an apparatus comprising Management Frames utilized in wireless communications (such as 802.11) associated with the apparatus, and the Management Frames being protection-capable or non-protection-capable and wherein said Management Frames indicate whether or not they are protection-capable. In one preferred embodiment of the present invention at least one of the Management Frames may be an Action Frame and the wireless communications can further include a Robust Security Network (RSN) Capabilities bit to be added for Action Frame protection negotiation and wherein the Action Frame protection negotiation may be provided by a Beacon/Probe Response source setting the RSN bit to indicate that protection is required for all protection-capable Action Frames.

[00032] If the RSN Capabilities bit is set to protection-capable, the Action Frames may be protected by applying the IEEE 802.11i CCMP protocol construction or the IEEE 802.11i TKIP protocol construction to the protection-capable Action Frames. Further, the CCMP protocol may use CCM to encrypt the Management Frame payload and to protect selected Management Frame header

fields from modification. The aforementioned apparatus may be a pair of wireless stations (STA) and wherein at least one of the pair of wireless stations (STA) may be an access point (AP).

[00033] In yet another embodiment of the present invention is provided a method of protecting Management Frames in wireless communications, comprising establishing the Management Frames as protection-capable or non-protection-capable, and protecting the Management Frames if the Management Frames are protection-capable. The step of protecting the Management Frames may further include adding a Robust Security Network (RSN) Capabilities bit to the Management Frames for Management Frame protection negotiation, wherein if the RSN Capabilities bit is set to protection-capable, the Management Frames may be protected by applying a protection protocol to the protection-capable Management Frames. The Management Frame protection negotiation may be provided by a Beacon/Probe Response source setting the RSN bit to indicate that protection is required for all protection-capable Action Frames. The protection protocol may be the IEEE 802.11i CCMP protocol construction or the IEEE 802.11i TKIP protocol construction. In one preferred embodiment of the present invention at least one of the Management Frames may be an Action Frame and wherein if the RSN Capabilities bit is set to protection-capable, the Management Frames may be protected by applying to the protection-capable Action Frames. The aforementioned CCMP protocol may use CCM to encrypt the Management Frame payload and to protect selected Management Frame header fields from

modification. Lastly, the TKIP protocol may use RC4 to encrypt the Management Frame payload and may use Michael, which is TKIP's message integrity algorithms, to protect selected Management Frame header fields from modification.

[00034] In yet another preferred embodiment of the present invention is provided an article comprising a storage medium having stored thereon instructions, that, when executed by a computing platform, establishes, in a wireless communication environment, protection-capable and non-protection-capable Management Frames, the protection-capable Management Frames being protected. Further, the protection-capable Management Frames being protected may be protected by adding a Robust Security Network (RSN) Capabilities bit to the Management Frames for Management Frame protection negotiation, wherein if the RSN Capabilities bit is set to protection-capable, the Management Frames may be protected by applying a protection protocol to the protection-capable Management Frames. The Management Frame protection negotiation may provided by a Beacon/Probe Response source setting the RSN bit to indicate that protection is required for all protection-capable Action Frames and the protection protocol may be the IEEE 802.11i CCMP or TKIP protocol construction.

[00035] While certain features of the invention have been illustrated and described herein, many modifications, substitutions, changes, and equivalents will now occur to those skilled in the art. It is, therefore, to be understood that the appended claims are intended to cover all such modifications and changes as fall

within the true spirit of the invention.